REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-15 and 17-26 are pending in the application. The Examiner additionally stated that claims 1-15 and 17-26 are rejected. By this communication, claims 1, 17, and 22 are amended. Hence, claims 1-15 and 17-26 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Objections

The Examiner objected to claim 1 because the claim recites "said keygen logickeygen unit." Appropriate correction was required.

In response, Applicant submits that the noted informality was perhaps an artifact of a poor scan resulting from a facsimile transmission. In reviewing the claim amendment as previously submitted, "keygen logic" was shown with a strikethrough, thus indicating that it was to have been deleted from the claim. The claim listing submitted herewith shows the desired language.

Accordingly, it is requested that the objection to claim 1 be withdrawn.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-6, 8-15, 17-20, and 22-25 under 35 U.S.C. 103(a) as being unpatentable over Yup et al. (US2002/0191784), hereinafter, "Yup," in view of Kessler et al. (US 6789147), hereinafter, "Kessler." Applicant respectfully traverses the Examiner's rejections.

As per claim 1, the Examiner noted that Yup discloses an apparatus for performing cryptographic operations, comprising:

- An instruction register having a cryptographic instruction, received by microprocessor as part of an instruction flow executing on said microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said one of the cryptographic operations (page 4, paragraph [0045]);
- A keygen unit, operatively coupled to said cryptographic instruction, configured to direct said microprocessor to load said user-generated key schedule (page 3, paragraph [0028]).
- An execution unit, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations, said execution unit comprising:
    - A cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (page 1, paragraph [0004]).

The Examiner conceded that Yup does not explicitly disclose that the device is microprocessor, but that Kessler discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2). The Examiner therefore concluded that it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup at al to be a processor, for one would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

As per claim 17, the Examiner opined that Yup discloses an apparatus for performing cryptographic operations, comprising:

- A cryptography unit within a microprocessor, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes a key size to be employed when executing said one of the cryptographic operations (AES block cipher can use varying key lengths) [page 4, paragraph 0045];
- A keygen unit, operatively coupled to said cryptography unit, configured to direct said microprocessor to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations (page 3, paragraph [0028].

The Examiner also noted that Yup does not explicitly discloses that the device is microprocessor, but that Kessler discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2) and, therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup et al to be a processor, noting that one would have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

As per claim 22, the Examiner wrote that Yup discloses a method for performing cryptographic operations in a device, the method comprising:

- Receiving a cryptographic instruction that prescribes employment of a user-generated key schedule during execution of one of a plurality of cryptographic operations (page 4, paragraph [0045]); and
- Employing the user-generated key schedule when executing the one of the cryptographic operations (page 3, paragraphs [0028-0035]).

The Examiner conceded that Yup does not explicitly disclose that the device is microprocessor, however, the Examiner noted that Kessler et al. discloses an interface for cryptographic processor, which further discloses a coprocessor (FIG. 2) and, therefore, it would have been obvious to one having ordinary skills in the art at the time the invention was made for the device described in Yup et al to be a processor, and that one would

have been motivated to use a processor in order to maximize system flexibility and to reduce space requirement for the design.

Responsive to Applicant's arguments submitted on 01/07/2008, the Examiner noted that they have been fully considered but they are not persuasive. The Examiner noted that the 102(e) rejection of claims 22-25 was due to an inadvertent typo, and that the rejection is an obviousness rejection under 103 over Yup in view of Kessler, and that the rejection is maintained in the instant office action.

The Examiner also noted that Applicant argued that "the microprocessor is not a coprocessor nor is a coprocessor a

microprocessor "see response at page 16. In reply, the Examiner stated that while a microprocessor is not a coprocessor (as asserted by Applicant), in the context of the claimed invention, they perform the same function. The Examiner pointed out that the claims merely recite a microprocessor for receiving a cryptographic instruction and thus the co-processor of Kessler does just that, and furthermore that the co-processor of Kessler includes an execution queue that fetches cryptographic instructions (Fig. 8) and therefore meets the claim limitation.

The Examiner also replied in response to Applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See In re Keller, 642 F.2d 413,208 USPQ 871 (CCPA 1981); In re Merck &Co., 800 F.2d 1091,231 USPQ 375 (Fed. Cir. 1986).

Applicant very much appreciates the Examiner's consideration of the previously submitted claim amendments, and the Examiner's response to Applicant's previously submitted arguments, in particular where it was pointed out that claims merely recite a microprocessor for receiving a cryptographic instruction and thus the co-processor of Kessler does just that.

Applicant has considered the Examiner's points and has thus amended claims 1, 17, and 22 to recite, substantially, that the microprocessor executes an *application program,* and that the cryptographic instruction is one of the instructions in the application program

which is fetched for execution. As one skilled in the art will concur, the capability to execute an application program, as opposed to executing single instructions or instruction threads which are handed off from a host microprocessor, is one of the significant distinctions between a microprocessor and a coprocessor. Accordingly, Applicant has amended the independent claims to recite that the microprocessor executes an application program, which clearly distinguishes the present invention over the circuit taught by Yup and the interface taught by Kessler.

Applicant submits that a single cryptographic instruction as part of an application program which is executed by a microprocessor according to the present invention is not contemplated by either one of the cited references, alone or in combination, for a co-processor is incapable of executing an application program (i.e., a co-processor only executes single instructions or instruction threads handed off from a host processor.) Applicant also asserts that the combination of the two references to perform cryptographic operations would not have led to the solution provided according to the present invention, but rather would have resulted *a coprocessor-based interface to a cryptographic coprocessor*, for this is what is taught by the two references in combination. Never is it contemplated, or even suggested, that a microprocessor capable of executing an application program be employed to execute a cryptographic instruction as part of the application program to perform a specified cryptographic operation because, at the time of invention, there was no existing mechanism that allowed for the execution of cryptographic operations by a general-purpose microprocessor other than via executing a complex and long series of instructions, typically obtained through an operating system call. In addition, it is further submitted that the teachings of Yup and Kessler in combination teach away from a host microprocessor based approach for performing cryptographic operations, for the suggestion of a separate circuit for performing cryptographic operations combined with a coprocessor interface leads one toward a cryptographic coprocessor implementation.

In contrast to the combined teachings of Yup and Kessler, Applicant realized that provision of an atomic cryptographic instruction for use in an application program and inclusion of a cryptographic unit within the execution logic of a microprocessor whereby

the cryptographic instruction could be executed as part of the operations performed when the microprocessor executes the application program would overcome the disadvantages associated with the approach resulting from a combination of the teachings of Yup and Kessler. It is thus a feature of the present invention to allow for use of the cryptographic instruction at the application level (i.e., within an application program as opposed to an operating system call), thus overcoming the disadvantages of present day coprocessor implementations.

Accordingly, it is requested that the rejections of claims 1, 17, and 22 be withdrawn.

With respect to claims 2-6 and 8-15, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a combination of Yup and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-6 and 8-15.

With respect to claims 18-20, these claims depend from claim 17 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a combination of Yup and Kessler. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 18-20.

Claims 23-25 depend from claim 22 and add further limitations that are neither anticipated nor made obvious by Yup, Kessler, or a combination of Yup and Kessler. Accordingly, Applicant respectfully submits that claims 23-25 are allowable as well.

The Examiner also rejected claims 7 and 21 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Kessler, and further in view of Miller (US 6081884), hereinafter, "Miller." Applicant respectfully traverses the rejections and notes that claims 7 and 21 depend from claims 1 and 17, respectively, and add further limitations over that subject matter which has been argued above as being allowable over the cited references. Accordingly, it is requested that the rejections of claims 7 and 21 be withdrawn.

The Examiner furthermore rejected claim 26 under 35 U.S.C. 103(a) as being unpatentable over Yup in view of Miller. Applicant respectfully traverses the rejection and notes that claim 26 depends from claim 22, and adds further limitations over that

subject matter which has been argued above as being allowable over the cited references. Accordingly, it is requested that the rejection of claim 26 be withdrawn.

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-15 and 17-26 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

07/16/2008

Date: _____